Technical Cybersecurity

Formatting your stack

Complexity++

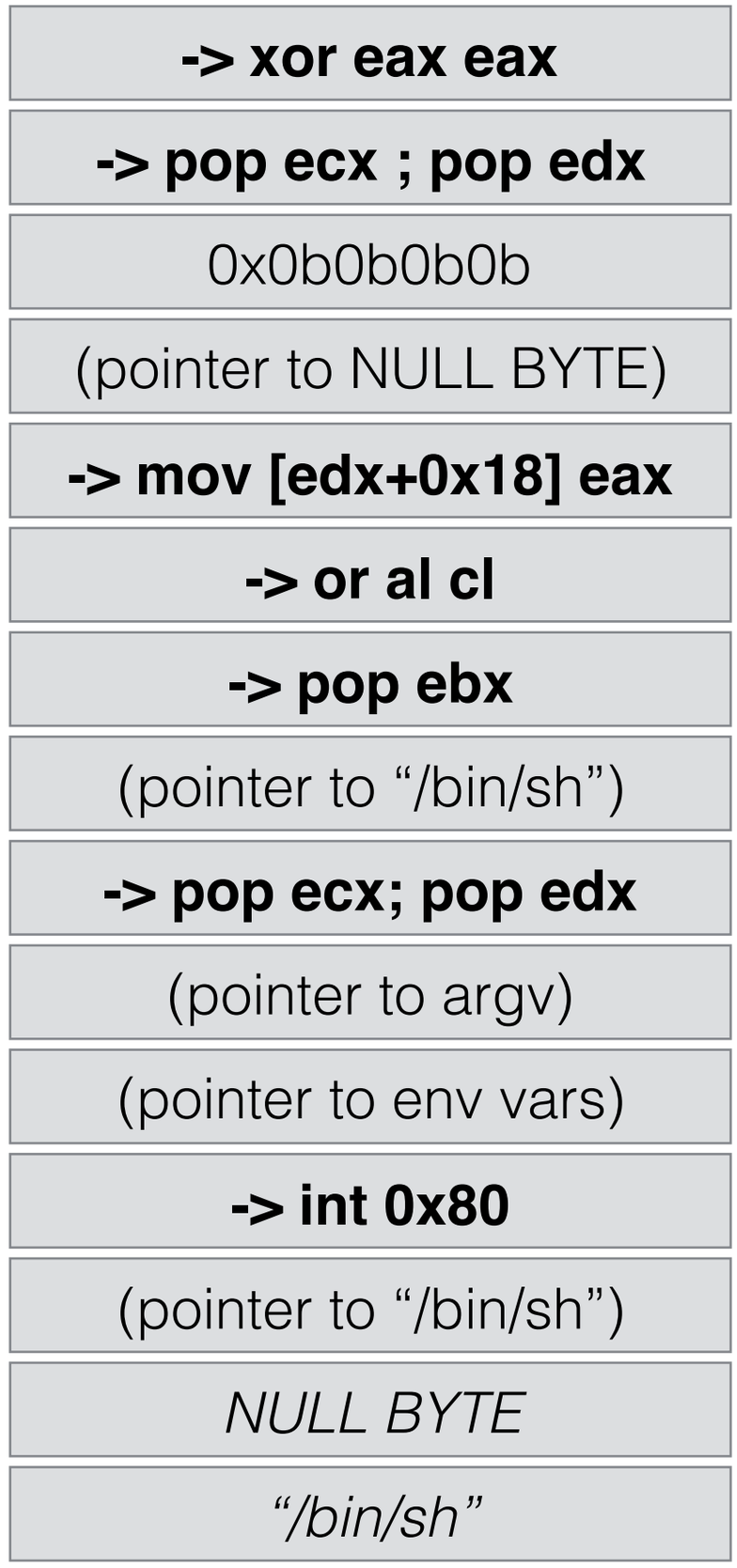
Stack formatting is much more difficult

- We need to move values into registers
  - 0x0b is the syscall number for **execve(.)**, must be in al
  - ebx must point to the string **execve(.)** will execute
  - ecx must point to the argv pointer array
  - edx must point to the envp array

Stack to Generate

VALUES & OPCODES

- You need to intersperse data with opcodes
- Data gets used during interpretation to create special byte arrangements



From here

Python program

- Create a python program to generate your stack to inject
  - We'd use the same approach, but at a much larger scale
  - Create, first, with recognizable bytes
- Send it to a file
- Read into the file at runtime
  - (gdb) r filename
  - $ rop filename
- Read and debug resulting core files

Modern exploitation is difficult!